EXHIBIT 3

1 CIT/ ES
JURY DEMAND

CAUSE NO. DC-24-20596

ALLAN ASKRENS, *on behalf of himself and all others similarly situated*, **Plaintiff,** **v.** **PALLET LOGISTICS OF AMERICA, LLC d/b/a PLA,** **Defendant.**	**IN THE DISTRICT COURT** **DALLAS COUNTY, TEXAS** 14th _____ **JUDICIAL DISTRICT**

PLAINTIFF'S CLASS ACTION PETITION

Plaintiff Allan Askrens, individually and on behalf of all others similarly situated ("Class Members"), brings this class action against Defendant Pallet Logistics of America, LLC d/b/a PLA ("Defendant" or "PLA"). The allegations set forth in this Petition are based on Plaintiff's personal knowledge as to his own actions and experiences, and upon information and belief and further investigation of counsel.

DISCOVERY CONTROL PLAN

Due to the complexity of this case, discovery should be conducted pursuant to a discovery control plan under Level 3, pursuant to Texas Rule of Civil Procedure 190.4. Plaintiff affirmatively pleads that this suit is not governed by the expedited actions process of Texas Rules of Civil Procedure 169 because Plaintiff seeks monetary relief in excess of $250,000.00.

NATURE OF THE ACTION

1. Defendant "is a leading provider of recycled pallets and pallet management services, handling more than 40 million pallets per year for over 500 customers."[1]

2. This action arises from a recent data breach (the "Data Breach") impacting highly sensitive employee data ("Private Information"), including Social Security numbers, in Defendant's possession.

3. The Data Breach occurred as a result of Defendant's failure to implement reasonable data security practices.

4. Plaintiff brings this action on behalf of himself and all others whose Private Information was compromised due to Defendant's failures.

5. Plaintiff and Class Members have suffered injuries because of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

---

[1] *See* Pallet Logistics of America, available at https://reusables.org/reusables-marketplace/pallet-logistics-ofamerica/#:~:text=Founded%20in%201989%20and%20headquartered,year%20for%20over%20500%20customers. (last accessed November 19, 2024).

6. Plaintiff brings this action on behalf of himself and all others similarly situated to remedy these harms and prevent a data breach of this nature from happening again.

PARTIES

7. Plaintiff Allan Askrens is and has been, at all relevant times, a resident and citizen of Bartlesville, Oklahoma. Plaintiff Askrens received the Notice Letter, via U.S. mail, from Defendant, dated November 12, 2024.

8. Defendant PLA is a Delaware corporation with its principal place of business located at 3030 Beltline Road, Suite 650, Addison Texas, 75001. Defendant is a citizen of Texas. For over 35 years, Defendant, "from [its] locations in Dallas, San Antonio, Hutchins, and Houston, TX and Oklahoma, OK" has "provide[d] new and recycled pallets and logistics solutions to manufacturers and retailers across Texas, Oklahoma, New Mexico, Colorado, Kansas, Missouri, Arkansas, Louisiana, and Mississippi."[2] It's registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

9. This Court has jurisdiction because Defendant's failure to adequately safeguard Plaintiff's and Class Members' data—*i.e.*, Defendant's negligent conduct—occurred in Dallas County, Texas. Plaintiff has been damaged in a sum within the jurisdictional limit, and pursuant to Texas Rule of Civil Procedure 47, Plaintiff seeks monetary relief over $1,000,000.00.

10. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in Dallas County, Texas. Venue is proper in Dallas County

[2] *See*, Pallet Logistics of America, available at https://www.plasolutions.com/pallet-logistics-of-america (last accessed November 19, 2024).

because Defendant's principal place of business is located in Dallas County and Defendant maintains Class Members' Private Information in Dallas County.

FACTUAL ALLEGATIONS

Defendant Pallet Logistics of America, LLC

11. Defendant is a limited liability company that provides pallets and logistics solutions. As a condition of employment, Defendant requires its prospective and current/former employees to provide their Private Information, including Social Security numbers.

12. Upon information and belief, Defendant requires its job applicants and employees to provide it with their sensitive Private Information as a condition of seeking and maintaining employment. Without this, Defendant would be unable to perform its regular business activities. Defendant retains this information even after the relationship has ended.

13. Upon information and belief, Defendant made promises and representations to its employees that the Private Information it collected from them as a condition of obtaining employment would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

14. It was with this reasonable expectation and mutual understanding that Plaintiff and Class Members provided their Private Information to Defendant. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. In turn, they relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

15. Defendant was obligated to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from involuntary disclosure and has a continuing legal duty to keep its employees' Private Information safe and confidential. Defendant recognizes these duties, declaring in its "Privacy Policy" last updated on April 4, 2023, that:

> "The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information."[3]

16. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without Plaintiff and Class Members providing Defendant this Private Information in exchange for being employed by Defendant, Defendant could not perform its business services.

17. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

Defendant's Data Breach

18. Over two months after discovering the Data Breach, on or about November 12, 2024, Defendant began sending Plaintiff and other victims of the Data Breach a Notice of Data Incident letter (the "Notice Letter"), informing them, in relevant part, that:

> Pallet Logistics of America d/b/a PLA ("PLA") is writing to inform you of a recent data security incident that may have involved your personal information. PLA takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your information, and offer you the opportunity

[3] *See* Privacy Policy, available at https://www.plasolutions.com/privacy#collecting-and-using-your-personal-data%C2%A0 (last accessed November 19, 2024).

to enroll in complimentary identity protection services that PLA is making available to you.

What Happened? On September 6, 2024, we discovered unusual activity in our digital environment. We immediately took steps to end this unusual activity and retained independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired limited files stored within our legacy systems (not our active systems). Upon learning this, we launched a comprehensive review of all potentially affected information to determine if any personal information was possibly acquired. Following the completion of this comprehensive review, we confirmed on October 18th 2024, that your personal information may have been involved in the incident. Since that time we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information was Involved? Following our review of the contents of the impacted data, on October 18th, 2024, we determined that your name and Social Security number or driver's license number were included. **We emphasize that we have no evidence of any actual or attempted misuse of this information**.

What Are We Doing? As soon as we discovered this incident, we took measures to further secure our network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information. Out of an abundance of caution, we are offering identity theft protection services through Identity Defense Complete, a data breach and recovery services expert. Identity Defense Complete identity protection services include 12 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, Identity Defense Complete will help you resolve issues if your identity is compromised.[4]

19. Although Defendant admits that names and Social Security numbers were affected—the most sensitive data a person has—it omitted from the Notice Letter any details about the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken to ensure such a breach does not occur again. Plaintiff and Class Members retain a

[4] Notice of Data Security Incident, PLA.

vested interest in ensuring that their Private Information remains protected; without these details, their ability to mitigate the harms resulting from the Data Breach is severely diminished.

20. Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, as evidenced by its offering Plaintiff and Class Members identity monitoring services. Yet, Defendant did not use reasonable security procedures and practices given the nature of the sensitive information it maintained, such as encrypting the information or deleting it when it is no longer needed.

21. The attacker accessed files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their Social Security numbers. Plaintiff further believes that their Private Information and that of Class Members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendant Acquires, Collects, & Stores Plaintiff's and Class Members' Private Information

22. As a condition of employment, Defendant requires its job applicants and employees to provide Defendant with their sensitive and confidential Private Information. Defendant retains this information and derives a substantial economic benefit from it. But for the collection of this Private Information, Defendant would be unable to perform its services.

23. By collecting this data, Defendant assumed legal and equitable duties and knew that it was responsible for protecting the Private Information from disclosure. Upon information and belief, Defendant made promises that it would maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

24. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to

make only authorized disclosures of this information. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

25. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is worsened by the repeated warnings and alerts directed at companies maintaining sensitive information to protecting and securing sensitive data.

Defendant Knew, Or Should Have Known, Of the Risk it Faced

26. Data thieves regularly target companies in possession of highly sensitive information. In storing the sensitive and confidential information of its job applicants, current, and past employees, Defendant should have reasonably recognized that Plaintiff's and Class Members' unprotected Private Information is valuable and could be highly sought after by cybercriminals.

27. It is widely known that Private Information, especially Social Security numbers, is a frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[5]

28. Indeed, cyber-attacks have become so widespread that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[6]

---

[5] *See* Identity Theft Resource Center's Annual End-of-Year Data Breach Report, available at https://www.idtheftcenter.org/post/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/ (last accessed September 4, 2024).

[6] *See*, Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, November 18, 2019, available at https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-

29. Defendant was aware of the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. Yet, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

30. Plaintiff's and Class Members' injuries were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for their Private Information. The ramifications are severe. Once Private Information is stolen, the fraudulent use of that information and coinciding damage may continue for years.

31. Given its voluntary taking of Plaintiff's and Class Members' confidential information, Defendant knew the importance of safeguarding that Private Information and the foreseeable consequences of a breach. This includes the significant costs imposed on Plaintiff and Class Members resulting from a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply With Industry Standards

32. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[7] To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

---

warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed April 17, 2024).

[7] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed April 17, 2024).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

33. All of these measures should have been employed, given that Defendant maintained the Private Information of employees. However, upon information and belief, Defendant failed to implement many of these safeguards, thus resulting in the Data Breach.

34. Additionally, experts studying cyber have identified several best practices that, at a minimum, should be implemented by companies in possession of sensitive Private Information, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these best practices, including a failure to implement multi-factor authentication.

35. Moreover, Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

36. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft

[8] *Id.* at 3-4.

37. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

38. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below. Here, the data stolen in the Data Breach has been used and will continue to be used in a variety of criminal ways to exploit Plaintiff and Class Members.

39. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[9] With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

40. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. This means that the

[9] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last accessed November 21, 2024).

Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this package can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

41. Following a data breach, reasonable victims are expected to take steps to mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

42. Recognizing the actual and imminent risk of identity theft faced by Plaintiff and Class Members, Defendant instructed Plaintiff and Class Members to take precautions, outlining recommended steps to take, in its Notice Letter.

43. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting Defendant to obtain more information about the Data Breach's occurrence, contacting financial institutions to sort out fraudulent charges on their accounts, and more.

44. These mitigation efforts are consistent with the U.S. Government Accountability Office 2007 report regarding data breaches that stated that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10] These

[10] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed April 17, 2024).

mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach.[11]

Diminution of Value of Private Information

45. Private Information is a valuable property right.[12] This value is axiomatic, considering the worth of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Undeniably, Private Information has considerable market value.

46. Private Information is highly useful to criminals, as evidenced by the monetary value attributed to stolen identity credentials on the dark web cited by numerous sources.[13] For example, Personal Information can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

47. Social Security numbers—which comprise some of the confidential information implicated in the Data Breach—are among the worst kind of Private Information to have stolen. This is because Social Security numbers can be used to achieve a variety of fraudulent uses and are difficult for an individual to change.

48. Obtaining a new Social Security number involves significant paperwork and evidence of actual misuse. Even then, this is not a guaranteed fix. According to Julie Ferguson of

---

[11] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed April 17, 2024).

[12] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last accessed April 17, 2024).

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed April 17, 2024).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed April 17, 2024).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed April 17, 2024).

the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

49. The information compromised in the Data Breach is more substantial than that of, for example, credit card information in a retailer data breach because, the information compromised in this Data Breach, like Social Security numbers, is impossible to "close" and difficult, if not impossible, to change. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[17] Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

50. Private Information can sell for as much as $363 per record according to the Infosec Institute.[18] Even consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[19]

---

[16] https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft#:~:text=%22The%20credit%20bureaus%20and%20banks,the%20victim%20of%20identity%20theft.%22 (last accessed November 21, 2024).

[17] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed April 17, 2024).

[18] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] Mike Brassfield, *This Company Will Pay You $50 This Year Just for Downloading Its Free App*, (updated May 31, 2019), available at https://www.thepennyhoarder.com/make-money/nielsen-panel/ (last accessed November 21, 2024).

51. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Because this information is now readily available, and its confidentiality lost, Plaintiff and Class Members have suffered an additional loss of value.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable And Necessary

52. Given the type of targeted attack in this case and the type of data involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

53. Such fraud may go undetected for years. An individual may not know that his Private Information was used to file for unemployment benefits until law enforcement notifies his employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

54. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

55. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When applying for employment and agreeing to work on Defendant's behalf, Plaintiff and other reasonable applicants and employees understood and expected that Defendant would properly safeguard and protect their Private Information. Accordingly, Plaintiff and Class Members received employment positions of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant's clients.

Plaintiff Allan Askrens' Experience

56. Upon Information and belief, Defendant obtained Plaintiff Askrens' Private Information when he applied to work for Defendant.

57. As a condition of obtaining employment with Defendant, Plaintiff was required to provide Defendant, directly or indirectly, with his Private Information, including his name and Social Security number. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

58. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

59. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated November 12, 2024, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach. According to this Notice Letter, Defendant's investigation "confirmed on October 18, 2024, that [Plaintiff's and Class Members'] personal information may have been involved in the incident."

60. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, communicating with his financial and insurance services providers to alert them of the breach and learn more about precautions he can take, and changing account passwords for all of his accounts tied to sensitive personal information. Plaintiff has spent significant time on activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

61. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

62. Plaintiff also suffered actual injury in the form of $4,000 in student loans that an unauthorized person applied for in his name in California, as well as experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

63. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

64. As a result of the Data Breach, Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

65. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

66. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

67. Pursuant to Texas Rule of Civil Procedure 42, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **The Class**
> All individuals whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach discovered by Defendant in or about September 2024 (the "Class").

68. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

69. Plaintiff hereby reserves the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery.

70. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,

upon information and belief in comprises thousands of individuals employed across the entirety of Defendant's network.

71. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

72. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

73. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

74. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

75. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

76. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

77. Likewise, particular issues under TRCP § 42(b)(3) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard employee Private Information; and

78. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Incident letters by Defendant.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

79. Plaintiff re-alleges and incorporate by reference all preceding allegations, as if fully set forth herein.

80. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of soliciting employees for its business, the services of which affect commerce.

81. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

82. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

83. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

84. Pursuant to the Texas Business and Commercial Code §§ 521.052 and 521.053, and industry standards, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' confidential Private Information from disclosure.

85. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

86. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being employed by Defendant.

87. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

88. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

89. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' Private Information it was no longer required to retain pursuant to regulations.

90. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

91. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

92. Defendant breached its duties, pursuant to the Texas Business and Commercial Code §§ 521.052 and 521.053, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former employees' Private Information it was no longer required to retain,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, even after discovery of the data breach.

93. Defendant's conduct violated the statutes referenced herein by failing to use reasonable measures to protect Private Information and comply with applicable industry standards, at described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

94. Plaintiff and Class Members are within the class of persons that the Texas Business and Commercial Code §§ 521.052 and 521.053 were intended to protect.

95. The harm that occurred as a result of the Data Breach is the type of harm these statutes were intended to guard against.

96. Defendant's violation of these statutes constitutes negligence.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable in light of Defendant's inadequate security practices.

98. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

99. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems. The injuries Plaintiff and Class Members suffered were also foreseeable.

100. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach. At the same time, Plaintiff and the Class had no ability to protect their Private Information that was in, and remains in, Defendant's possession.

101. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

102. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

103. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

104. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

105. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered (and will continue to suffer) injuries, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information. As a result of these injuries, Plaintiff and Class Members are entitled to compensatory, nominal, and/or consequential damages.

106. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

107. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Invasion of Privacy (Public Disclosure of Private Facts)
(On behalf of Plaintiff and the Class)

108. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

109. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

110. As a result of Defendant's conduct, publicity was given to Plaintiff's and Class Members' Private Information.

111. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' Private Information to be highly offensive.

112. Plaintiff's and Class Members' Private Information is not of legitimate public concern and should remain private.

113. As such, Defendant's conduct, as alleged above, resulted in a public disclosure of private facts, for which it is liable.

114. As a direct and proximate result of Defendant's publication of their private facts, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial and any other relief allowed by law.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Class)

115. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

116. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiff's and Class Members.'

117. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as a necessary part of being employed by Defendant or otherwise seeking employment from Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

118. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

119. As such, a portion of the revenue derived from its employees is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

120. Defendant, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

121. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

122. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

123. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

124. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own

profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

125. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

126. Plaintiff and Class Members have no adequate remedy at law.

127. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information.

128. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

129. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

130. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

131. Plaintiff and Class Members directly contracted with Defendant.

132. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of seeking and/or being employed by Defendant.

133. Plaintiff and Class Members reasonably understood that, in exchange for providing and/or seeking employment from Defendant, that Defendant would pay for adequate cybersecurity measures from a portion of their revenues.

134. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

135. Plaintiff and the Class Members accepted Defendant's offers by disclosing their Private Information to Defendant in exchange for employment. In turn, and through internal policies, Defendant agreed to protect and not disclose Private Information to unauthorized persons.

136. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information. After all, Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

137. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

138. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair

dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

139. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

140. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to adequatelysafeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

141. In these and other ways, Defendant violated its duty of good faith and fair dealing.

142. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

143. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

144. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of putative Class Members as defined above, respectfully request that this Court:

A. Certify this case as a class action, appoint Plaintiff as the Class Representative, and appoint the undersigned as Class Counsel;

B. Order appropriate relief to Plaintiff and the Class;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

F. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all triable issues.

Dated: November 21, 2024

Respectfully submitted,

/s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000
214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Terence R. Coates*
MARKOVITS, STOCK & DE MARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Counsel for Plaintiff and the Proposed Class
**Pro Hac Vice* application forthcoming

FORM NO. 353-3 CITATION

THE STATE OF TEXAS

To: PALLET LOGISTICS OF AMERICA, LLC D/B/A PLA
BY SERVING ITS REGISTERED AGENT CT CORPORATION SYSTEM
1999 BRYAN ST SUITE 900
DALLAS TX 75201

GREETINGS:
You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. on the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. In addition to filing a written answer with the clerk, you may be required to make initial disclosures to the other parties of this suit. These disclosures generally must be made no later than 30 days after you file your answer with the clerk. Find out more at TexasLawHelp.org. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Dallas, Texas 75202.

Said Plaintiff being **ALLAN ASKRENS**

Filed in said Court **21st day of November, 2024** against

PALLET LOGISTICS OF AMERICA, LLC D/B/A PLA

For Suit, said suit being numbered **DC-24-20596,** the nature of which demand is as follows:
Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.
Given under my hand and the Seal of said Court at office **on this the 30th day of November, 2024**

ATTEST: FELICIA PITRE,
Clerk of the District Courts of Dallas County, Texas

By __/S/CHARISMA PRESTON__, Deputy
CHARISMA PRESTON

ESERVE

CITATION

No.: DC-24-20596

ALLAN ASKRENS
vs.
PALLET LOGISTICS OF AMERICA, LLC

ISSUED
on this the 30th day of November, 2024

FELICIA PITRE
Clerk District Courts,
Dallas County, Texas

By: **CHARISMA PRESTON**, Deputy

Attorney for Plaintiff
JOE KENDALL
3811 TURTLE CREEK BLVD
SUITE 825
DALLAS TX 75219-4693
214-744-3000
jkendall@kendalllawgroup.com

DALLAS COUNTY
SERVICE FEES
NOT PAID

OFFICER'S RETURN

Cause No. DC-24-20596

Court No.: 14th District Court

Style: ALLAN ASKRENS
vs.
PALLET LOGISTICS OF AMERICA, LLC

Came to hand on the _____day of _____, 20_____, at _____o'clock _____.M. Executed at _____, within the County of _____ at _____ o'clock _____ .M. on the _____day of_____, 20_____, by delivering to the within named _____

_____

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by me in serving such process was _____miles and my fees are as follows: To certify which witness my hand.

For serving Citation $_____ _____

For mileage $_____ of_____ County, _____

For Notary $_____ By_____ Deputy

(Must be verified if served outside the State of Texas.)

Signed and sworn to by the said_____ before me this_____ day of _____, 20_____, to certify which witness my hand and seal of office.

_____

Notary Public_____ County_____

NINA MOUNTIQUE
CHIEF DEPUTY

CAUSE NO. DC-24-20596

ALLAN ASKRENS

vs.

PALLET LOGISTICS OF AMERICA, LLC

14th District Court

ENTER DEMAND FOR JURY

JURY FEE PAID BY: ALLAN ASKRENS

FEE PAID: $10.00

FILED
12/30/2024 9:30 AM
FELICIA PITRE
DISTRICT CLERK
DALLAS CO., TEXAS
Margaret Thomas DEPUTY

Cause No. DC-24-20596

Allan Askrens, on behalf of himself and all others similarly situated,	§	**IN THE DISTRICT COURT**
***Plaintiff*,**	§	
	§	**DALLAS COUNTY, TEXAS**
v.	§	
	§	
Pallet Logistics of America, LLC dba PLA	§	**14TH JUDICIAL DISTRICT**
***Defendant*.**	§	

DEFENDANT'S ORIGINAL ANSWER AND AFFIRMATIVE DEFENSES

In accordance with the Texas Rules of Civil Procedure, Defendant Pallet Logistics of America, LLC d/b/a PLA ("Defendant" or "PLA") serves *Defendant's Original Answer and Affirmative Defenses* ("Answer") in response to *Plaintiff's Class Action Petition* ("Petition") filed by Plaintiff Allan Askrens ("Plaintiff" or "Askrens"). In support, Defendant shows the following:

I.
GENERAL DENIAL

1. Defendant enters a general denial of all material allegations contained in Plaintiff's *Petition* in accordance with Tex. R. Civ. P. 92.

II.
AFFIRMATIVE DEFENSES

Without assuming any burden of proof Defendant does not otherwise bear, and reserving the right to amend its *Answer* to assert additional defenses that may become known during these proceedings, and as otherwise allowed by the Texas Rules of Civil Procedure and orders of this Court, Defendant asserts the following affirmative and other defenses:

2. Plaintiff's recovery, if any, is limited by his failure to mitigate his damages, if any.

3. In accordance with Texas Civil Practice and Remedies Code § 41.0105, Defendant asserts that Plaintiff's recovery of medical or healthcare expenses, if any, is limited to the amount actually paid or incurred by or on behalf of Plaintiff.

4. Defendant invokes Chapter 41 of the Texas Civil Practice & Remedies Code

concerning all claims of gross negligence and exemplary damages, including but not limited to: § 41.003(b) clear and convincing evidence burden of proof; § 41.003(a) and § 41.001(7)(b) definition of culpable acts or omissions; § 41.003(c) proximate causation; § 41.003(d) requiring a unanimous finding by the jury as to liability and amount of exemplary damages; § 41.007 limitation on recovery and pre-judgment interest; § 41.009 bifurcation for the trial of these issues; and § 41.008 regarding limitation of recovery for exemplary damages.

5. Plaintiff should not recover any exemplary damages because any such award would: (1) violate the Excessive Fines clause of the Eighth Amendment of the United States Constitution by failing to place a limit on the amount; (2) be void for vagueness and violate the Equal Protection clause of the Fifth and Fourteenth Amendments of the United States Constitution; (3) violate Article 1, §§ 13 and 19 of the Constitution of the State of Texas; or (4) violate due process.

6. Defendant contends that Plaintiff's claim for prejudgment interest is limited by the dates and amounts set forth in Chapter 304 of the Texas Finance Code, and any other applicable statute.

7. Plaintiff's claims are barred to the extent they involve any transactions or events, or seek any damages for any periods outside any applicable statutory limitations period.

8. Plaintiff's damages, if any, are limited by the statutory provisions under which they are brought.

9. Plaintiff's damages, if any, are barred under the economic loss doctrine.

10. Defendant asserts that to the extent Plaintiff has received benefits from collateral sources or other setoffs or recoupments, Plaintiff's alleged damages, if any, must be diminished accordingly.

11. Plaintiff's damages, if any, were caused by his own conduct or by the conduct of third parties.

12. Plaintiff's request for equitable relief is barred under the doctrine of laches, estoppel, waiver, or unclean hands.

III.
CONCLUSION AND PRAYER

Upon trial of this action, Defendant prays that this Court enters judgment that Plaintiff take nothing by his claims, awards Defendant its costs of court and any recoverable attorney's fees, and grants any further relief to which the Court determines Defendant is justly entitled.

Respectfully submitted,

CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

/s/ Brent Sedge
Brent Sedge
Texas Bar No. 24082120
bsedge@constangy.com
1201 Elm Street, Suite 2550
Dallas, TX 75270
214.646.8970

ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

In accordance with Texas Rule of Civil Procedure 21a, I certify that I served *Defendants Original Answer and Affirmative Defenses* on December 30, 2024, ***via eServe*** on the following individuals:

Joe Kendall (jkendall@kendalllawgroup.com)
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, TX 75219

Terence R. Coates (tcoates@msdlegal.com)
MARKOVITS, STOCK & DE MARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202

ATTORNEYS FOR PLAINTIFF

/s/ Brent Sedge
Brent Sedge

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Brent Sedge on behalf of Brent Sedge
Bar No. 24082120
bsedge@constangy.com
Envelope ID: 95703450
Filing Code Description: Original Answer - General Denial
Filing Description: Defendant's Original Answer and Affirmative Defenses
Status as of 12/30/2024 9:33 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
JOE KENDALL		jkendall@kendalllawgroup.com	12/30/2024 9:30:44 AM	SENT

14TH DISTRICT COURT
GEORGE L. ALLEN, SR. COURTS BUILDING
600 COMMERCE STREET, ROOM 360
DALLAS, TEXAS 75202-4606
Chambers of JUDGE ERIC V. MOYÉ

December 30, 2024

File Copy

DC-24-20596 ALLAN ASKRENS vs. PALLET LOGISTICS OF AMERICA, LLC

ALL COUNSEL OF RECORD AND PRO SE PARTIES:

Please take note of the following settings:

Jury Trial - Civil November 18, 2025 9:30 AM

THIS IS A LEVEL 3 CASE. THE PARTIES SHOULD PREPARE AN AGREED SCHEDULING ORDER **(WHICH MUST INCLUDE A MEDIATOR)** AND SUBMIT IT TO THE COURT WITHIN 30 DAYS OF THIS NOTICE. IF NO AGREEMENT IS REACHED, PLEASE ADVISE THE COURT.

Trial announcements must be made in accordance with Rule 3.02, Dallas Civil Court Rules.

When no announcement is made for defendant, defendant will be presumed ready. If plaintiff fails to announce or to appear at trial, the case will be dismissed for want of prosecution in accordance with Rule 165a, Texas Rules of Civil Procedure.

Plaintiff/Plaintiff's counsel shall serve a copy of this notice on any currently named defendant(s) answering after this date.

Sincerely,

ERIC V. MOYÉ
DISTRICT JUDGE
14TH DISTRICT COURT

Required scheduling order format available:
https://www.dallascounty.org/government/courts/civil_district/14th/StandardOrders.php

Cc:
BRENT DOUGLAS SEDGE
1201 ELM STREET SUITE 2550
DALLAS TX 75270

JOE KENDALL
3811 TURTLE CREEK BLVD SUITE 825
DALLAS TX 75219-4693